AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

United States of America
v.
Andrew Venegas

Case No. **4:23-mj-1417**

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May 15, 2022 in the county of Harris in the Southern District of Texas, the defendant(s) violated:

Code Section	*Offense Description*
18 USC 2251	Sexual Exploitation of Children

This criminal complaint is based on these facts:

See Attached Affidavit.

☑ Continued on the attached sheet.

Complainant's signature

John Bamford, FBI Task Force Officer
Printed name and title

Sworn to before me by telephone

Date: 07/12/2023

Judge's signature

City and state: Houston, Texas

Christina A. Bryan, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN THE MATTER OF: §
Andrew Venegas §

Case No. **4:23-mj-1417**

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, John Bamford, being duly sworn, depose and state:

1. I am a police officer with the Arlington County Police Department, which is in Virginia, and have been so employed since 2008. I am currently assigned as a Task Force Officer with the Federal Bureau of Investigation. In this role, I investigate computer-related crimes. As such, I have participated in numerous investigations involving computer and high technology related crimes, including computer intrusions, online extortion, online threats, Internet fraud, credit card fraud, and bank fraud. I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States. I have had the opportunity to observe and review numerous examples of child pornography in all forms of media including computer media. Child Pornography, as defined in 18 U.S.C. § 2256, is:

   "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . [or] (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct." For conduct occurring after April 30, 2003, the definition also includes "(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct."

2. This Affidavit is made in support of a criminal complaint charging Andrew Venegas with violating Title 18 U.S.C. § 2251(a) – sexual exploitation of children, more specifically defined as:

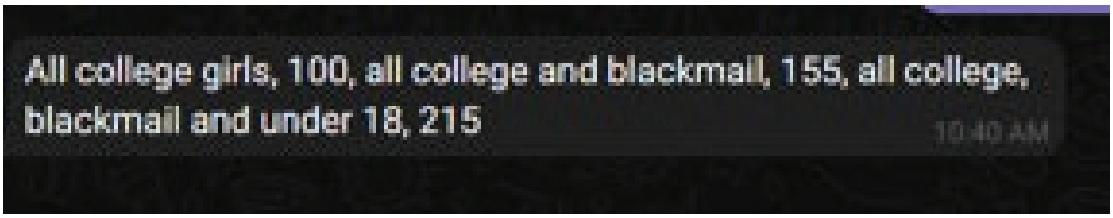
"Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed."

3. I am familiar with the information contained in this Affidavit based upon the investigation I have personally conducted and my conversations with other law enforcement officers involved in this investigation, or who have engaged in numerous investigations involving child pornography.
4. Because this Affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation, I have set forth only those facts that I believe are necessary to establish probable cause that evidence of a violation of Title 18 U.S.C. § 2251(a) has been committed by Andrew Venegas on or about May of 2022 within the Southern District of Texas. Where statements of others are set forth in this Affidavit, they are set forth in substance and in part.

Summary of Probable Cause

5. Since at least the summer of 2022, Andrew VENEGAS (hereafter VENEGAS) is believed to have obtained and attempted to obtain explicit images and videos of women and used digital media to extort women throughout the United States. Additionally, VENEGAS is believed to have provided such material to others to do the same, utilizing the online moniker "Starkylol." VENEGAS interacted with victims throughout the United States and sold content to law enforcement during the investigation. He advertised his content to other

individuals online, including specifically offering content depicting minors under the age of 18. The image below depicts a conversation between VENEGAS (using the moniker Starkylol) and law enforcement in which VENEGAS advertised the images he had available for sale.



6. Although VENEGAS took numerous steps to obfuscate his identity, law enforcement was able to identify him using records from a number of various electronic providers, as detailed below.

Probable Cause

Investigation into VENEGAS as a Poster on Specific Websites

7. I and other law enforcement officers are investigating a scheme by which individual(s) are utilizing websites (TARGET DOMAINS) which offer nude, sexually suggestive, and/or sexually explicit images for view or sale. Some of these images appear to have been obtained from unauthorized access to victims' social media accounts. Numerous victims have reported to law enforcement that they did not authorize anyone to take the nude, sexually suggestive, and/or sexually explicit images from their account, and at least one victim reported that some of the images or videos in their account depict them when they were a minor.

Background

8. The investigation of the websites at the TARGET DOMAINS began with an investigation into TARGET DOMAIN A. Law enforcement began to investigate TARGET DOMAIN A after the Alexandria, Virginia Police Department requested assistance. During the investigation, I learned that the TARGET DOMAIN A website posted sexually explicit, sexually suggestive, and/or nude images of females in various stages of undress. The website itself mentions the unlawful intrusion into Snapchat accounts as a service offered on the site. Numerous victims throughout the country have reported that their images or

videos were posted on TARGET DOMAIN A without their permission. Some of the victims specifically reported that they believed the images/videos were taken from their Snapchat account without their permission.

9. Many victims sought out assistance from local police departments. Several victims first found out that their images or videos were posted after individuals contacted them and threatened to share the images/videos with friends or family if they did not provide additional explicit images and videos. Additionally, at least one victim reported that some of the sexual images depicted them as a minor. Moreover, law enforcement identified several additional potential victims whose posted images appear to depict them when they were minors. Law enforcement identified several victims who reported that images of them were taken without their permission and whose images were posted on TARGET DOMAIN A.

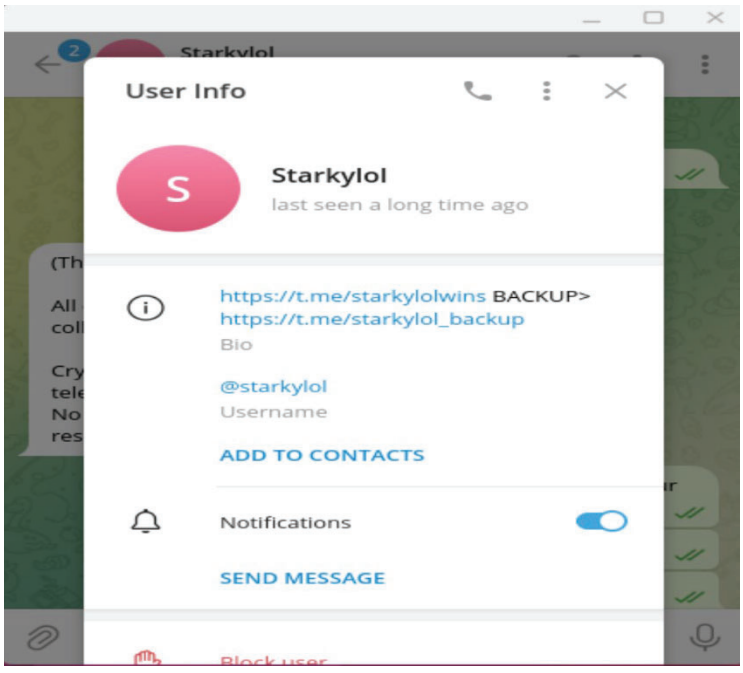
10. During the investigation, it was discovered that photographs of victims were either separately or concurrently being posted on TARGET DOMAIN B. The two websites hosted at DOMAIN A and DOMAIN B have almost identical names (with only one letter distinguishing them), indicating a possible common administrator(s). TARGET DOMAIN B also has a similar overall appearance to the TARGET DOMAIN A website. For example, the two webpages have a similar webpage design, and both feature young females in various states of undress and/or engaged in sexual acts. TARGET DOMAIN B, much like TARGET DOMAIN A, allows users to search based upon state or their name and posts the full names of many of the young females. However, unlike on the TARGET DOMAIN A webpage, where clicking on a female's page featured on the site allowed a user to view either the images or smaller "thumbnails" of the images, the TARGET DOMAIN B webpage directs the user to a login page for a VIP account. Although many of the images are not fully visible without the VIP account, the viewable images on the website often show the victim either in various stages of undress and/or engaged in sexual conduct, and often include the face of the victim. Analysis of the two websites has resulted in law enforcement believing that over 1000 different females had their images posted on the website, often accompanied by their true names.

Identification of Starkylol

11. During the investigation of the TARGET DOMAINS, law enforcement discovered that many of the images posted on the websites had been "watermarked" with various phrases. Law enforcement believes that such "watermarks" are a way to denote the original poster or who obtained the original images.
12. At least some of the images were found to contain the watermark "TELEGRAM Starkylol." Law enforcement knows that Telegram is an encrypted messaging application. Based upon my training and experience, it therefore appeared that Starkylol was the Telegram username for a person who obtained or posted the images.
13. From on or about February of 2023 through the time of this writing, law enforcement investigators have been able to purchase numerous images of various females which bore a watermark reading "TELEGRAM Starkylol."

Examination of Starkylol on Telegram

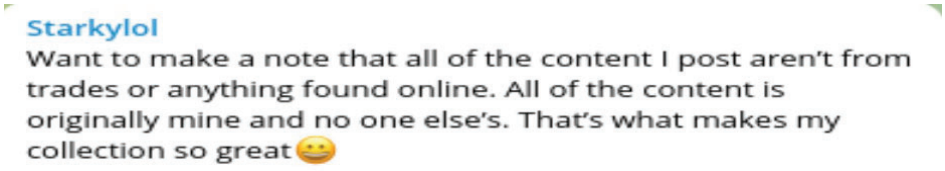
14. Law enforcement discovered an account on Telegram in the name of Starkylol. A review of this account shows that Starkylol provides "channels" which are located on his account information page (see below image):



15. Law enforcement reviewed the channel which had the URL https://t.me/starkylolwins. On the channel, various still photographs and video clips were viewable of various females clothed, in stages of undress, and engaged in sexually explicit activities. Along with these

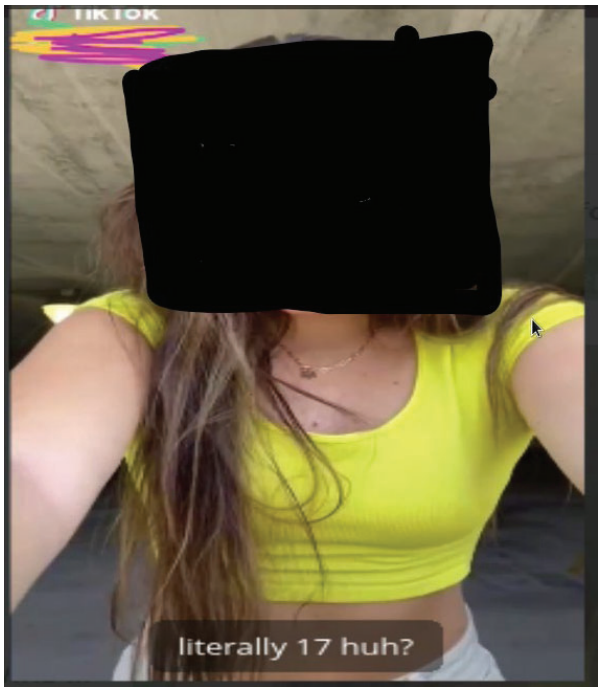
images were posts made on the channel by the account owner, believed to be Starkylol. Below are descriptions of some of the images viewable on the channel, statements made by Starkylol, and (when available) the date that the images were posted:

a. A post by Starkylol claims that all of the images found on his channel were the result of him obtaining them:

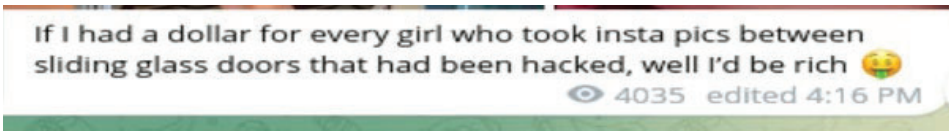


b. On September 22, 2022, a video containing an individual identified by law enforcement as Minor Victim 5 (MV-5) was posted onto the channel. In this post, MV-5 appears to be nude (topless but her vagina was not visible) and she appears to be masturbating or simulating masturbating against a pillow or cushion. Law enforcement knows MV-5 was a minor at the time of the video's creation and at the time the video was posted, and is currently under the age of 18. As further explained below, MV-5 was being extorted by VENEGAS to commit the sexual acts shown in the video. I first observed the video on or about May 16, 2023.

c. A post, dated on September 22, 2022, shows two images. The first is of what appears to be a TikTok video clip of a female (the TikTok user's name has been obscured by the poster). The image included the words "literally 17 huh?" (see below with the female's face obscured by law enforcement). Along with this image was a second image of a person who appears to be the same female, this time nude, facing the camera with her legs spread exposing her vagina and breasts. Of note, while law enforcement has not been able to identify the female in these images, the post stating "literally 17" and her appearance suggest that this victim was under the age of 18 at the time of the photo.



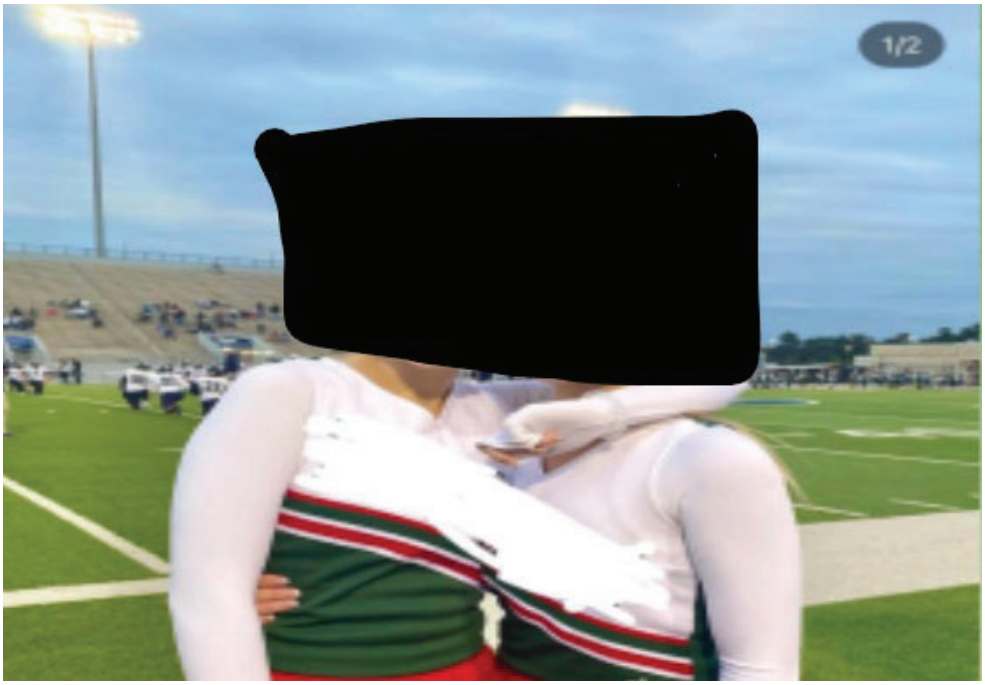
d. Another post contained two images of an unknown female. In one image, the female individual is in a bikini style bathing suit, while in the other, she is simulating oral sex on the handle of a hairbrush. Underneath this image was a post stating below:

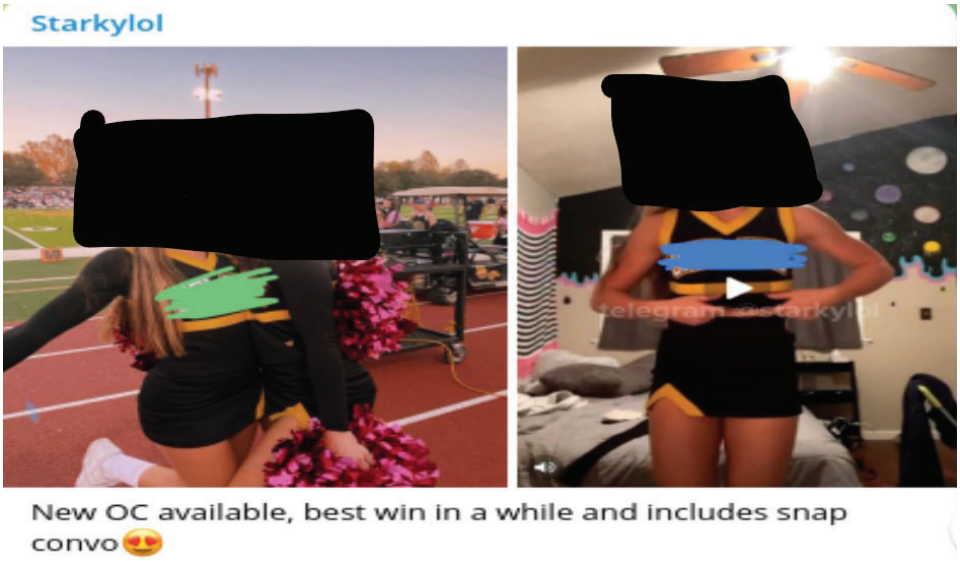


e. Another post included two images, one of a fully clothed female while the other depicted what appears to be the same female engaged in oral sex. Along with these images, the post stated "why can't every girl have a video like this in their my eyes only [crying face emoji]." I know from training and experience that the term "my eyes only" is a reference to Snapchat's service called "My Eyes Only," which is a file storage system that encrypts the files so they are not accessible except through the account. Based upon victim interviews, often the images found on the TARGET DOMAINS were obtained without authorization from the "My Eyes Only" section of the victim's Snapchat account.

f. Other posts include images of various females that appear to be under the age of 18. Such images depict teenaged females in high school cheerleading outfits (the

actual name of the school was obscured on the image similar to how the TikTok username was obscured above).[1] Examples are included below, with the faces obscured by law enforcement. The second image also includes a written post by Starkylol which references "OC" and "snap." Based on my training, experience, and investigation, I understand these references to refer to "original content" and chats held on the Snapchat app, respectively.

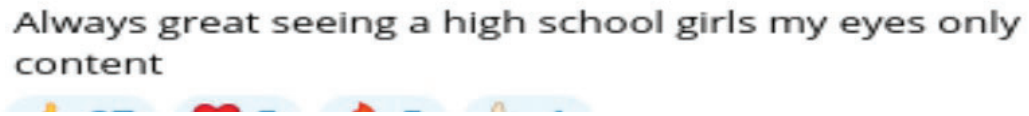




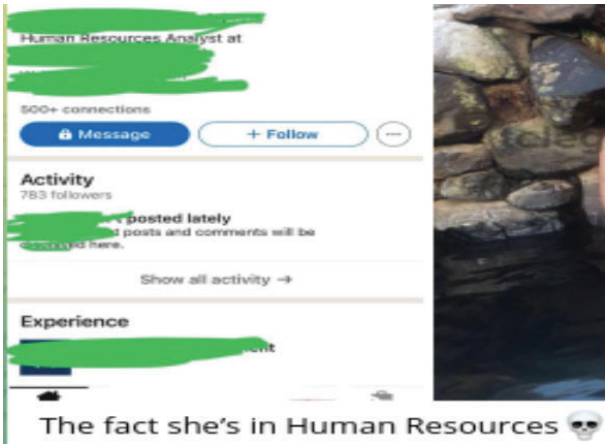
[1] The belief that the images depict high school cheerleaders is based upon the background size of the football stadium (smaller bleachers) and apparent age of the females captured in the images.

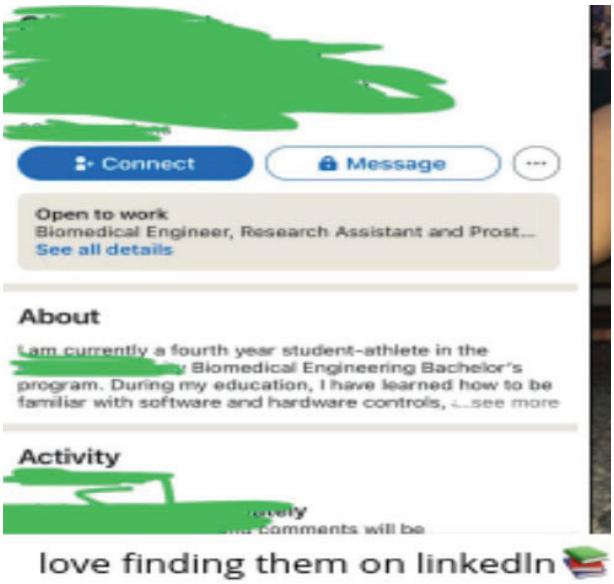
g. Another post references "bm" (believed to be shorthand for "blackmail") and provides the name of a victim (redacted by law enforcement). Additionally, based on my training, experience, and investigation, I know the use of the ghost emoji refers to Snapchat, because app uses the ghost as part of its logo.

h. Another post references videos of high schoolers engaged in sexual intercourse, followed by a post referencing both high school girls and "My Eyes Only":

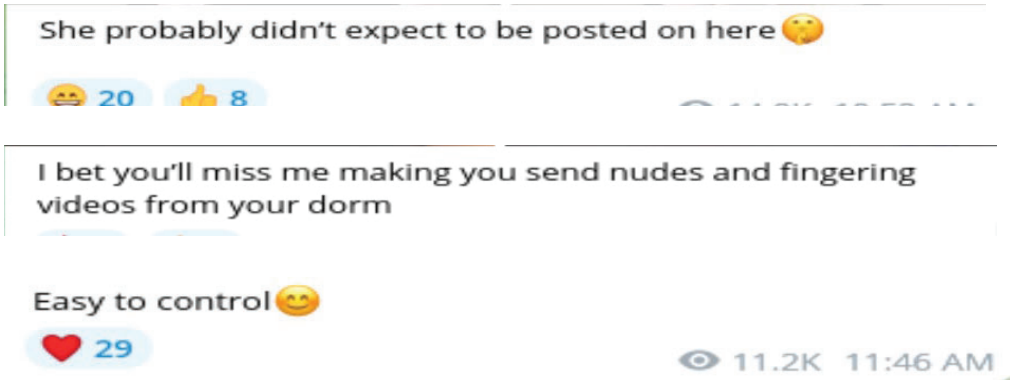


i. Two other posts describe how Starkylol targets female victims. These posts depict screenshots of what appears to the be the professional networking site LinkedIn:





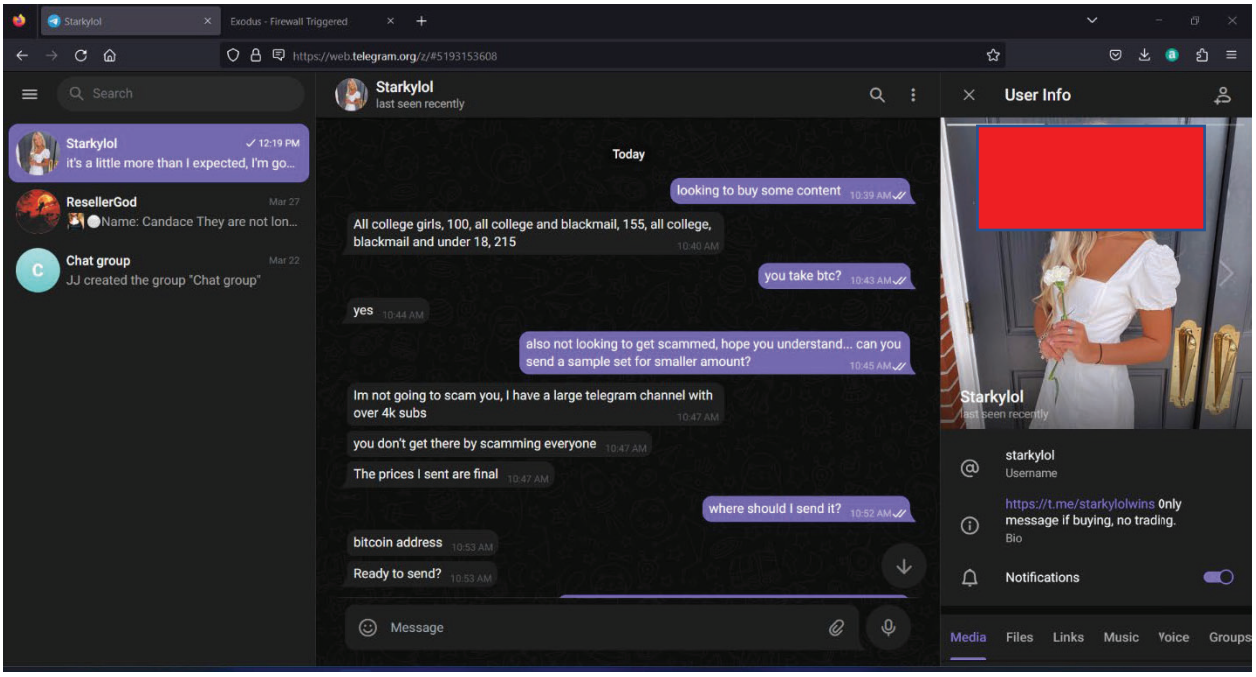
j. Other posts suggest, based upon their language, that Starkylol was knowingly forcing women to create and/or provide images against their will or that the images were posted without their consent:



Attempted Purchase from Starkylol Number 1

16. On February 17, 2023, law enforcement, acting in an undercover capacity, contacted Starkylol using the messaging app Telegram. Starkylol provided prices for various types of content, specifically (as depicted above) "All college girls, 100, all college and blackmail, 155, all college, blackmail and under 18, 215." Based on the context and my training and experience, I believe Starkylol is offering sets or packages of images. He is charging $100 for a set of all of the images of "college girls", $155 for images of college girls, along with the contact information that would be necessary to blackmail them for additional images, and $215 for all college girls, their contact information, and images of

minors. The initial conversation part of the conversation is set forth in the below screenshot. Of note, the image to the right is the profile picture used by Starkylol and is of a yet to be identified female:



2

17. The UC attempted to negotiate a lower price and mentioned a fear of being "scammed." Starkylol responded by stating he had over 4000 followers and one did not develop that type of following by not providing the content.

18. Law enforcement purchased, utilizing cryptocurrency (bitcoin), the package purporting to contain "all college, blackmail and under 18" and, while in the Eastern District of Virginia, conducted a partial download before Starkylol canceled the download, claiming that the UC had taken too long to download the material. Law enforcement was able to obtain some images from Starkylol that were provided in file folders of what were believed to be the names of the females depicted. Additionally, law enforcement downloaded other folders that did not contain images but still had the names of the females. During this investigation, law enforcement did not request any new content be created by Starkylol, rather, as shown above, requested content already available from Starkylol.

[2] Face of unknown female was redacted.

19. Starkylol provided the UC with access to the images by providing a link to the file-sharing platform called mega.nz.

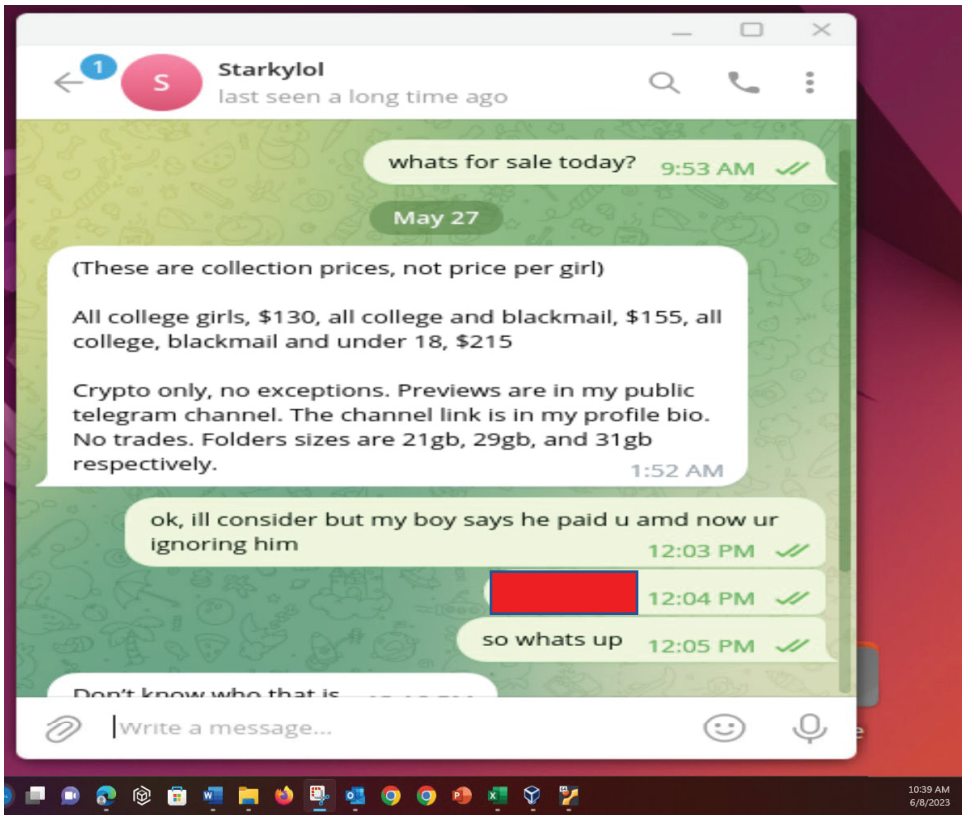
20. Records provided by mega.nz show that the images were provided by an account created with the email of starkylol@protonmail.com.

Attempted Purchase from Starkylol Number 2

21. On or about May 23, 2023, law enforcement, acting in an undercover capacity using a new username, contacted Starkylol using the messaging application Telegram. Starkylol again provided the prices for content, stating that "All college girls, $130, all college and blackmail, $155, all college, blackmail, and under 18, $215."

22. The UC sent virtual currency (bitcoin) to an address provided by Starkylol to purchase the content. Starkylol never provided the content and refused to respond to any inquiries by the UC to obtain the content.

23. On or about May 26, 2023, law enforcement, using a third moniker, reached out to Starkylol and inquired about what he was selling. On or about May 27, 2023, Starkylol provided the following response depicted in the screen capture below:



24. As of the date of this writing, law enforcement has still not received the content from the second attempted purchase nor the full content from the first purchase.

Attempt to Identify Victims of Starkylol[3]

Identification of MV-5

25. During the review of Starkylol's Telegram Channel, law enforcement discovered two posted videos of a female under the age of 18 who has been identified as MV-5. In one of the videos, MV-5 appears to be nude (topless but her vagina was not visible) and she appears to be masturbating or simulating masturbating against a pillow or cushion. Her full face was observed in at least part of the video. Furthermore, images of MV-5 were purchased by law enforcement from TARGET DOMAIN B. A watermark with the wording "telegram starkylol" was clearly visible on many of the images. The files purchased included not only images of MV-5 but also screenshots of the conversation between MV-5 and VENEGAS, from VENEGAS's point of view, to include images sent to VENEGAS. MV-5 provided law enforcement a recording of some of the same conversation but from MV-5's point of view.

26. Law enforcement interviewed MV-5, who is a minor female that has resided in the Southern District of Texas at all relevant times of the offense and investigation. MV-5 provided a recording of communications between herself and VENEGAS (at one point provided the Telegram moniker Starkylol).[4] MV-5 stated that the initial intrusion and subsequent conversations happened around May of 2022. The following was learned:

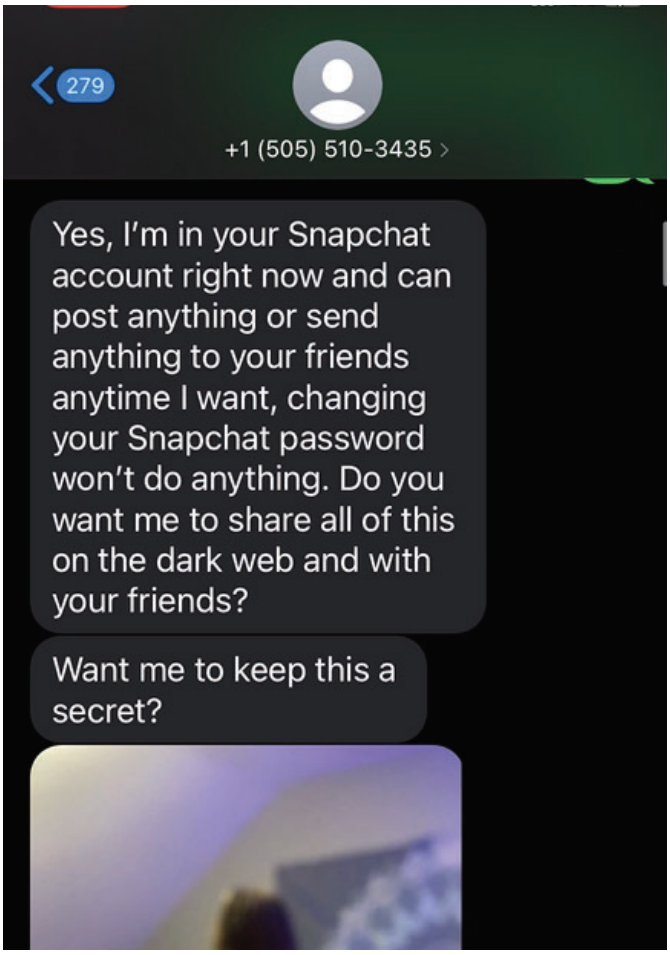
    a. MV-5 was contacted by a phone number, 505-XXX-3435. Of note, this same

[3] A Virginia local law enforcement agency has obtained the contents of a Snapchat account believed to be utilized by Starkylol to communicate with at least some females. In some of the communications, it appears that the person believed to be Starkylol attempted to confirm that the women were at least 18 years old.

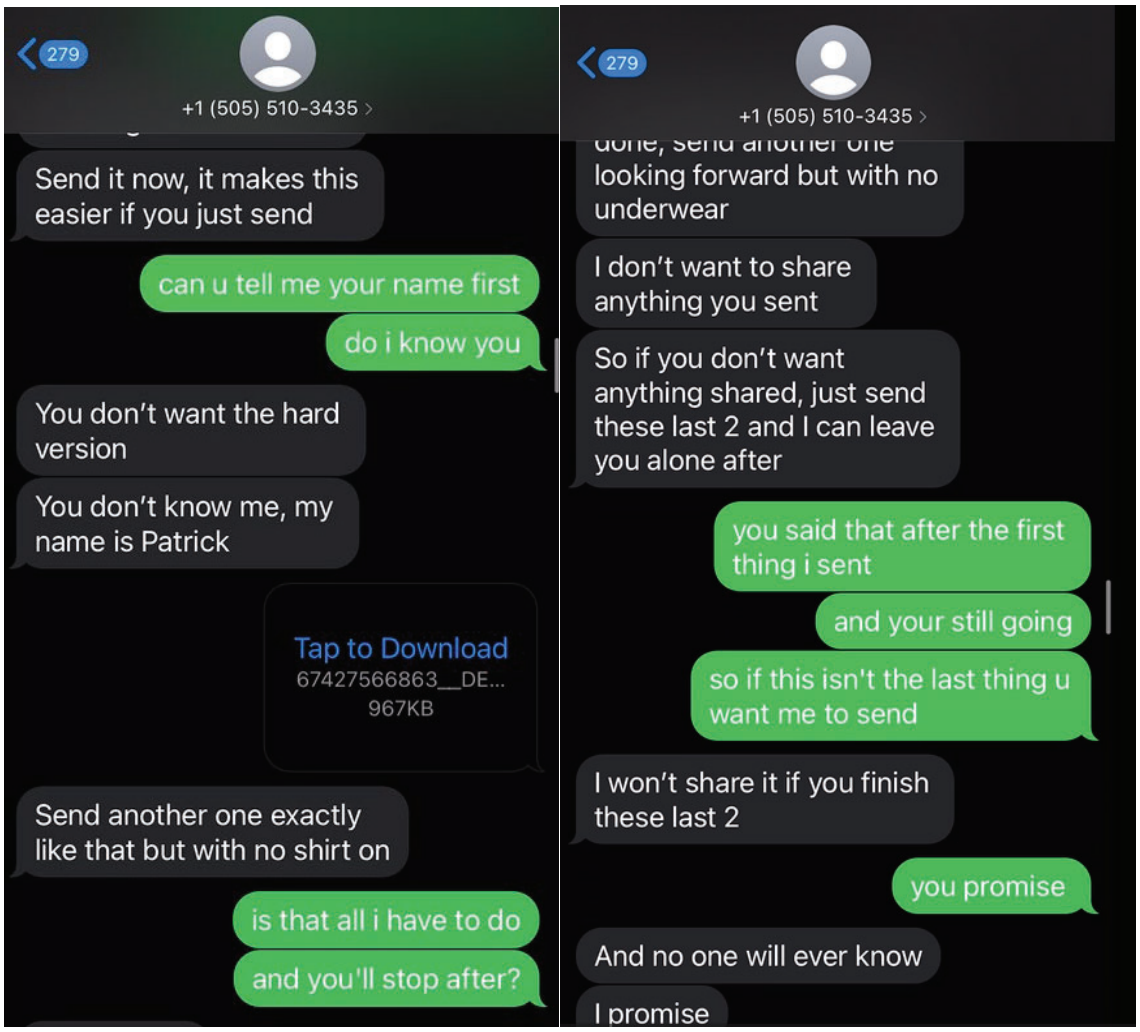
[4] MV-5 was able to provide the screen recording of the text messages between herself and VENEGAS but not of the conversation between VENEGAS and herself via Telegram.

number contacted AV-8 as discussed below.

b. As shown in the below message, VENEGAS told MV-5 that he had gained access into her social media account. In the message sent to MV-5, VENEGAS included the account information of MV-5's social media account, which included her listed birthdate. MV-5's birthdate clearly shows that she was under the age 18 at the time of these messages. Along with the statement that is included below, he sent images to MV-5 from her Snapchat Account of her in various stages of undress (she appears to be wearing underwear in most of the images). See below image:

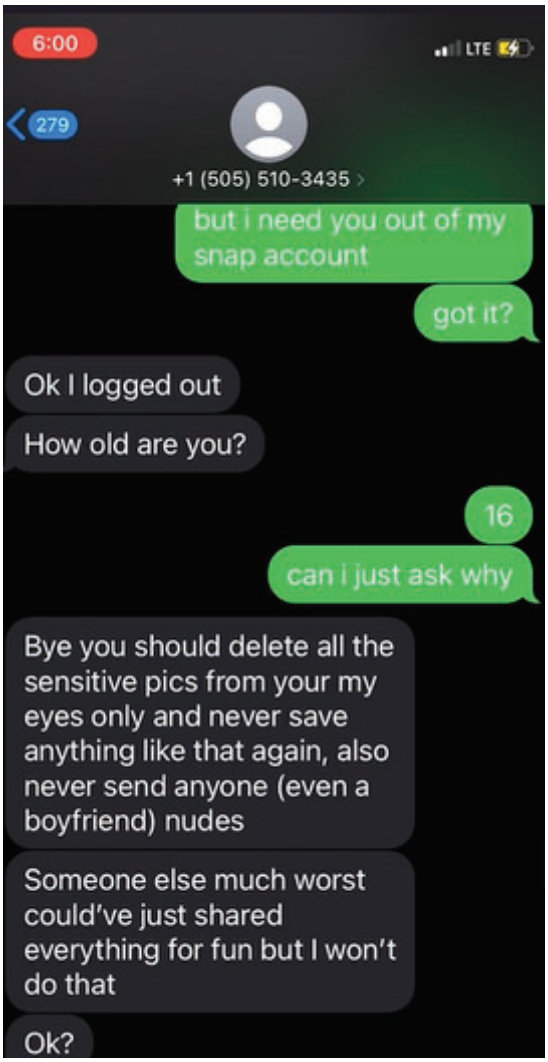


c. After this post, Venegas made MV-5 create videos and images in various stages of undress. Examples of this is shown below:



d. During the conversation, VENEGAS had MV-5 bend over while naked and take an image. This same conversation was found in the files obtained by TARGET DOMAIN B along with the image described. This image shows a female, believed to be MV-5, bent over with her vagina and anus clearly visible.

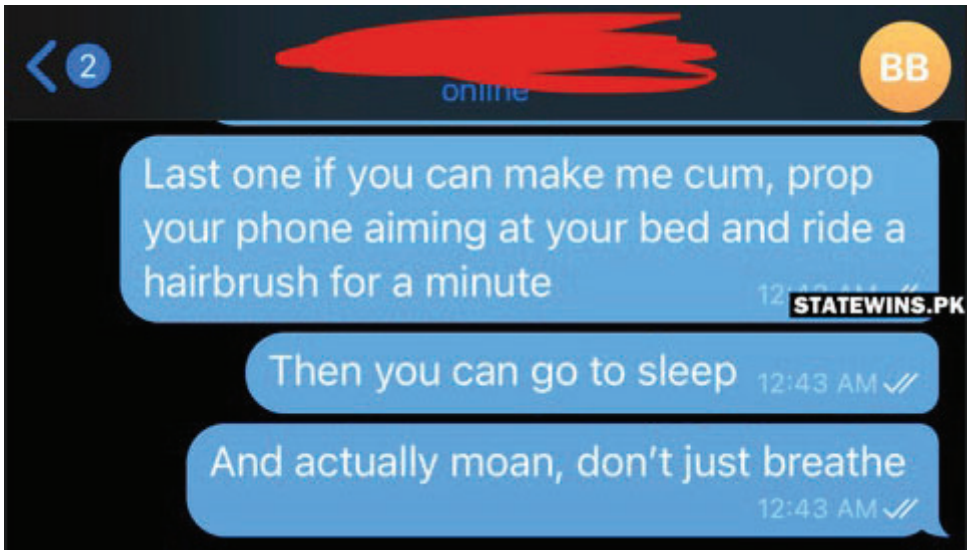
e. During the conversation, VENEGAS asked MV-5 how old she is and she states she is 16. This part of the conversation is shown below:



f. At the end of the recording, VENEGAS has MV-5 create a Telegram account and provides her the moniker @starkylol to contact him on.

27. Additionally, images obtained from TARGET DOMAIN B show a conversation between MV-5 and VENEGAS on Telegram.

g. During this conversation, images of MV-5 masturbating while nude with her face visible were shown. Additionally, during the conversation, VENEGAS tells MV-5 to penetrate herself with a hairbrush and film herself. See below:



h. Based upon the files obtained from TARGET DOMAIN B, this appears to be when the video of MV-5 masturbating or simulating masturbation found on Starkylol's Telegram channel was created.

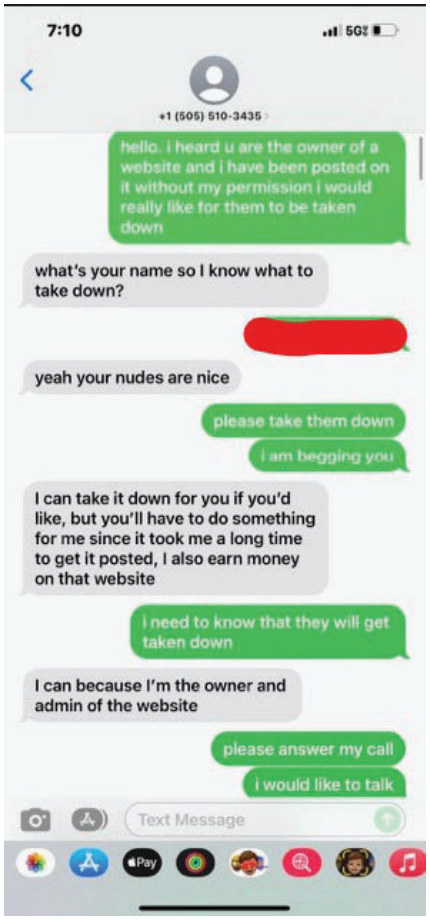
Identification and Interview of Adult Victim 8 (AV-8)

28. In May of 2022, a victim (AV-8) who resides in California, reported that her social media account was illegally accessed and nude and sexually explicit images of hers were stolen and posted onto TARGET DOMAIN A.

29. After this occurred, an unknown individual contacted her through a social media account and advised that the owner of TARGET DOMAIN A was using the phone number 505-XXX-3435 (hereafter phone number 3435). The unknown individual, who purported to be a female, claimed to have also been victimized and had their pictures posted online. The unknown individual appears to have deleted the social media account used to contact AV-8, but AV-8 captured screenshots of the conversation and provided them to law enforcement.

30. AV-8 contacted phone number -3435 and stated the images were posted without her permission and she wanted them to be taken down. AV-8 provided law enforcement this

initial conversation as a screenshot which is below, to include AV-8's statement "please take them down I am begging you." [5]



31. As shown above, the person using the number of -3435 stated that AV-8 would have to do something for them since they earn money via the TARGET DOMAIN B website. AV-8 asked what would be needed to take the images down, and the user of -3435 stated that AV-8 would have to pay them or send the user of -3435 more pictures. AV-8 offered $200, and the user of -3435 countered and demanded $250 in virtual currency (bitcoin) to take down the images. In order to make the payment, the user of -3435 provided Victim with a bitcoin wallet address ending in -7VAx and instructed AV-8 to send the money there. AV-

[5] AV-8 identified herself to the user of -3435 but her name was obscured in the image provided.

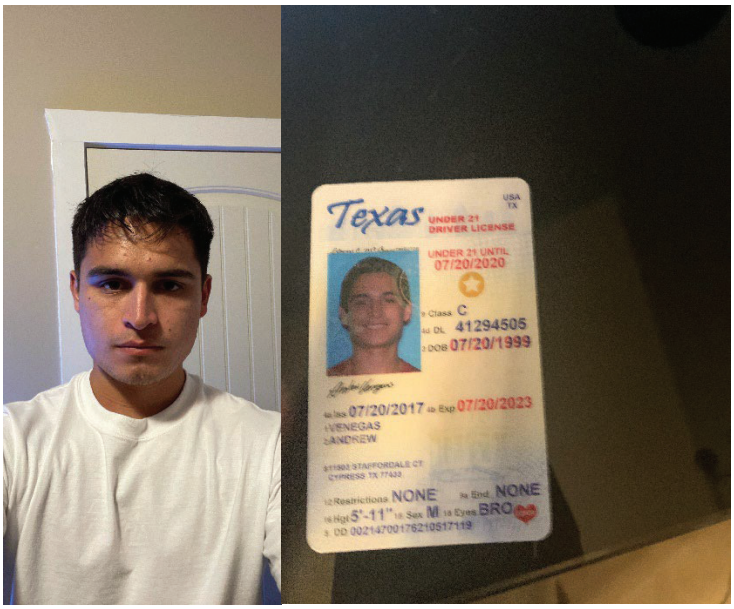
8 paid, transferring approximately .0083731 bitcoin to the wallet ending -7Vax. There is no evidence that the images were ever removed; in fact, law enforcement was able to purchase the images from TARGET DOMAIN B and also received the images in the purchase made directly from Starkylol.

Tracing of California Victim's Payment to Starkylol and VENEGAS's Cryptocurrency Account

32. Law enforcement discovered that the wallet ending in -7VAx was maintained by a cryptocurrency company (Company 1) and received records indicating that the owner of the bitcoin wallet ending in -7VAx created the account on or about February of 2022 using two emails: starkylol@protonmail.com (the same as the email used to create the Mega.nz account discussed above) and andrewx135790000@gmail.com.

33. Additionally, the records included transactional data pertaining to the movement of virtual currency. These records reflect that within an hour of AV-8's payment to wallet -7Vax, almost the exact same amount of bitcoin (.0083733 bitcoins) was transferred out of the -7Vax wallet to a wallet at a second cryptocurrency company (Company 2).

34. Records provided by Company 2 showed that the money was transferred to an account in the name of "Andrew Venegas." The account was registered to the email account running072099@icloud.com. Additionally, the registrant had provided a driver's license and photo as part of the registration process. The driver's license is for Andrew VENEGAS, and the image appears to be of the same person pictured in the driver's license.



35. A review of Company 1 and Company 2 records show that from approximately February to June 2022, the controller of these two accounts conducted numerous transactions where virtual currency (bitcoin) of similar amounts, approximately $200 dollars, was transferred from the Company 1 account to VENEGAS's Company 2 account. While the records provide different time periods and amounts for the transfer, law enforcement was able to determine that these transactions are the same because each transaction has the same transaction hash for both accounts. A transaction hash is similar to being a virtual currency version of a paper receipt—it shows that a particular transaction, i.e. exchange of the virtual currency, was validated and added to the blockchain ledger. The transactions described are not the only transactions from these accounts. Company 1 records show that virtual currency as removed from the account a total of 49 times and that 13 times, virtual currency was sent directly from the Company 1 account to VENEGAS's Company 2 account. The amount of the transaction values likely differ as a result of the fees taken by both companies.

36. Additionally, a review of other payments into VENEGAS's Company 2 account show at

least one payment that, based upon the comment that accompanied the transaction, is believed to be a payment similar to the undercover payment made by law enforcement in its undercover purchase. Specifically, on or about January 29, 2022, virtual currency was transferred to VENEGAS's Company 2 account by another account. Along with this transfer, the other account holder included a comment which stated, "for high school chick and college athlete." Based upon the advertisement for content that was shown above, law enforcement believes that this payment was for photos and/or videos of victims who were in high school and college.

Google Records

37. Law enforcement obtained records from Google pertaining to the email account of andrewx135790000@gmail.com, which was one of the two email addresses associated with the Company 1 account. This email account listed the name of the subscriber as "Andrew V" and provided the recovery email running072099@icloud.com, which is the same email utilized to register VENEGAS's Company 2 account discussed above.

38. Additionally, Google records show that various payment cards were associated with the Google account of andrewx135790000@gmail.com. Many of the located payment cards are in the name of Andrew Venegas. Other payment cards located within the account were cards that are believed to belong to a suspected family members of VENEGAS (hereby referred to as A.V. and M.V.).

Apple Records

39. Law enforcement obtained records from Apple pertaining to the aforementioned email address of running072099@icloud.com. Subscriber information for this account provides that the residential address of this account was the TARGET ADDRESS. The name on the

account is provided as first name "Nj" while the last name is "V."

40. Additionally, the Apple records provided the name of the person pertaining to transactions related to the account. Three different names related to the transactions with the most common ones being Andrew Venegas or Drew V, a less common name was M.V. who is believed to possibly be a family member of VENEGAS.

41. Additionally, it should be noted that the numbers within the email address of running072099@icloud.com are in fact VENEGA's date of birth (July 20, 1999).

Analysis of IP Addresses

42. On February 10, 2023, both the Apple account and the Company 2 account linked to VENEGAS were accessed via the IP Address of 2.57.169.146. Additionally, this same IP Address was captured by Company 1 to access his account as discussed above.

43. The email address of andrewx135790000@gmail.com was accessed from IP addresses 2600:1700:3930:cca0:79c4:4a92:4338:fd95 and 2600:1700:3930:cca0:7d56:3c36:507e:b67d. These two IP addresses were assigned by AT&T to an account registered in the name of A.V.[6]

44. The Mega.nz account of Starkylol@protonmail.com was accessed via the IP addresses of 2600:1700:3930:cca0:b8ed:aef7:7cad:df56 and 2600:1700:3930:cca0:d0ff:2b2b:8d55:2f90. These IP Addresses were also issued by AT&T to an account registered in the name of A.V.

45. Additionally, as stated above, the IP Address of 45.31.117.107 was also utilized to access accounts linked to VENEGAS (the explanation showing the linkage is put forth below) to

[6] This name was provided in full in the AT&T records but was abbreviated in this document by law enforcement. A.V. is the same name as found in the Google records discussed above and is the name of a suspected family member of Venegas.

include the starkylol@protonmail.com Mega.nz account on October 15, 2022, the email account of andrewx135790000@gmail.com account on October 21, 2022, and the Apple account linked to the email address of running072099@icloud.com between the dates of October 18, 2022, through May 15, 2023. This overlap and longevity suggest, along with the fact that the Internet Serve Provider being ATT, that this IP Address is likely a residential IP Address. [7]

IP Address Link to TARGET ADDRESS

46. As mentioned above, at least some of the IP addresses were associated with an AT&T account held by A.V. The address on the account was the TARGET ADDRESS. More specifically:

    i. On or about April 10, 2023, the mega.nz account associated with the email address of starkylol@protonmail.com was accessed via an IP address that, at that time, was assigned to A.V.'s account.

    j. On or about March 28, 2023, the mega.nz account associated with the email address of starkylol@protonmail.com was accessed via an IP address that, at that time, was assigned to A.V.'s account.

    k. On or about March 5, 2023, the Google account of Andrewx135790000@gmail.com was accessed via an IP address that, at that time, was assigned to A.V.'s account.

Search Warrant at 26811 Vizcaya Park Drive (VENEGAS Residence)

47. On or about July 12, 2023, a search warrant was executed upon the residence of 26811 Vizcaya Park Drive, Magnolia, Texas, which is the residence of VENEGAS. During the execution of the search warrant, law enforcement located a cellular phone in VENEGAS's bathroom. The search warrant was issued on July 11, 2023, by the Honorable Sam S.

[7] At the time of this writing law enforcement has not yet received records from ATT for this IP Address.

Sheldon of the United States District Court for the Southern District of Texas.

48. The cellular phone had notifications turned on and, as a result, received messages were visible on the screen. I observed that at least some of the messages were received on the Telegram Messaging Application.

49. While in the Target Residence, I sent two messages from an undercover Telegram Account to the account of Starkylol. Both those messages were displayed on VENEGAS's phone. I know from my training and experience that this means that the phone was receiving messages as Starkylol. This observation, in conjunction with the information as set for above, establish probable cause to believe that VENEGAS is Starkylol.

50. Based upon the information delineated above, I believe that probable cause exists for the issuance of a Criminal Complaint charging Andrew Venegas with a violation of Title 18 U.S.C. § 2251(a) - the sexual exploitation of children.

_____
John Bamford
Task Force Officer, FBI

Subscribed and sworn to before me, via telephone, this 12th of July 2023 and I find probable cause.

_____
Christina A. Bryan
United States Magistrate Judge